

Construction of Unit-Memory MDS Convolutional Codes

Chin Hei Chan and Maosheng Xiong

Abstract

Maximum-distance separable (MDS) convolutional codes form an optimal family of convolutional codes, the study of which is of great importance. There are very few general algebraic constructions of MDS convolutional codes. In this paper, we construct a large family of unit-memory MDS convolutional codes over \mathbb{F}_q with flexible parameters. Compared with previous works, the field size q required to define these codes is much smaller. The construction also leads to many new strongly-MDS convolutional codes, an important subclass of MDS convolutional codes proposed and studied in [8]. Many examples are presented at the end of the paper.

Index Terms

Convolutional code, unit-memory code, maximum-distance separable (MDS) codes, strongly-MDS codes, Reed-Solomon code, free distance.

I. INTRODUCTION

The class of convolutional codes was invented by Elias in 1955 [4] and has been widely in use for wireless, space, and broadcast communications since the 1970s. However, compared with the theory of linear block codes, convolutional codes are not so well understood. In particular, there are only a few algebraic constructions of convolutional codes with good designed parameters.

Let \mathbb{F}_q be the finite field of order q where q is any prime power. Let $\mathcal{F} := \mathbb{F}_q((D))$ be the field of Laurent series over \mathbb{F}_q . Following [18], a q -ary rate k/n and degree δ convolutional code, or an $(n, k, \delta)_q$ code for short, is a k -dimensional subspace of \mathcal{F}^n over \mathcal{F} with degree δ . It is known that δ is an invariant and is the external degree of a minimal encode that realizes the convolutional code (see also [13], [17]).

Let \mathcal{C} be an $(n, k, \delta)_q$ code and let d_{free} be the free distance of \mathcal{C} . The four parameters $n, k, \delta, d_{\text{free}}$ are of fundamental importance because k/n is the rate of the code, δ and d_{free} determine respectively the decoding complexity and the error correcting capability of \mathcal{C} with respect to some decoding algorithms such as the celebrated Viterbi algorithm [23]. For these reasons, for given rate k/n and q , generally speaking, it is desirable to construct convolutional codes with relatively small degree δ and relatively large free distance d_{free} . The generalized Singleton bound for an $(n, k, \delta)_q$ convolutional code \mathcal{C} , in its most general form, proposed and proved by Rosenthal and Smarandache [19], states that the free distance d_{free} of \mathcal{C} must satisfy

$$d_{\text{free}} \leq (n - k) \left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right) + \delta + 1. \quad (1)$$

If the inequality is attained as an equality, then \mathcal{C} is called a maximal-distance-separable (MDS) convolutional code. As in the classical case, MDS convolutional codes form an optimal family of convolutional codes, the study of which is of great importance.

For any rate k/n and any degree δ , Rosenthal and Smarandache [19] established the existence of $(n, k, \delta)_q$ MDS convolutional codes over some finite field \mathbb{F}_q by techniques from algebraic geometry without giving explicit constructions. Then in a beautiful follow-up paper [21], building upon ideas from Justesen [14], the authors provided an explicit construction of MDS convolutional codes for each rate k/n and each degree δ over some \mathbb{F}_q . However, in their construction, a relatively large field size q is required: it is necessary that $n|(q-1)$ and $n \leq \frac{q-1}{2}$. Hence the question was raised by the authors as to whether or not it is possible to come up with new constructions of MDS convolutional codes so that the field size q can be reduced and the condition $n|(q-1)$ can be dropped.

In this paper we provide a partial but affirmative answer to this question. Roughly speaking, we construct unit-memory $(n, k, \delta)_q$ MDS convolutional codes for any rate k/n and relative small but flexible δ as long as $n \leq q+1$, hence the strength of the result is almost comparable to that of classical MDS linear block codes over \mathbb{F}_q . Moreover, a nice feature of the construction is that many of the codes constructed satisfy a much stronger MDS condition: they are actually “strongly-MDS” convolutional codes, an important subclass of MDS convolutional codes proposed and studied by Gluesing-Luerssen, Rosenthal and Smarandache in [8]. We summarize our results as follows.

Theorem 1. *Let q be any prime power.*

- (i). There exists an $(n, k + \delta, \delta)_q$ MDS convolutional code for any $q \geq 3$ and positive integers n, δ, k such that $2\delta + k \leq n \leq q$.
- (ii). There exists an $(n, k + \delta, \delta)_q$ strongly-MDS convolutional code for any $q \geq 3$ and positive integers n, δ, k such that $3\delta + k - 1 \leq n \leq q$.
- (iii). If $q > 2$ is even, then there exists a $(q + 1, q + 2 - 2k - \delta, \delta)_q$ MDS convolutional code for any positive integers k, δ such that $\delta + k \leq \frac{q+1}{2}$.
- (iv). There exists a $(q + 1, k + 2\delta, 2\delta)_q$ strongly-MDS convolutional code for any $q \geq 5$ and positive integers k, δ such that $6\delta + k \leq q + 2$.

We remark that (i) and (ii) of Theorem 1 summarize Theorem 3 in Section III and Theorem 4 in Section IV; (iv) summarizes Theorems 5 and 7 in Section V; (iii) is obtained by using Theorem 6 in Section V and Lemma 4 in Section II. It shall be noted that in (ii) and (iv) the codes also have a maximum distance profile. Interested readers may review these theorems for details.

It was proved in [8, Theorem 3.11] that for every positive integers n, k, δ such that $n - k$ divides δ and for every prime number p there exists a strongly-MDS code with parameters (n, k, δ) over a suitably large field of characteristic p , and it was conjectured (see [8, Conjecture 3.13]) that for all $n > k > 0$ and for all $\delta \geq 0$ there exists an $(n, k, \delta)_q$ code over a sufficiently large field which is both strongly-MDS and has a maximum distance profile. (ii) and (iv) of Theorem 1 can be considered as a small step further toward this conjecture.

In this paper we only consider construction of unit-memory MDS convolutional codes, usually over a large alphabet, but this class of codes should be of great interest both in theory and in applications. First, unit-memory convolutional codes (UMC) are an interesting class of convolutional codes because their block length can be chosen to agree with the word length of computers or microprocessors that are used in the coding and decoding process. Lee [15] suggested that short binary UMC's are attractive with Viterbi decoding as the inner coding component of a concatenated system. Thommesen and Justesen [22] further derived bounds on the distance profile and free distance of binary UMC's and suggested that UMC's may have superior properties. Ebel [3] has made a thorough discussion on various methods in search of UMC's with good parameters. Second, as was pointed out in [8], a convolutional code over a finite alphabet can be practically identified with a finite linear state machine (LFSM) which has redundancy and which is capable of correcting processing errors. In a series of recent papers [9]–[11], Hadjicostis and Verghese showed how to error protect a given LFSM with a larger redundant LFSM capable of detecting and correcting state transition errors, and the construction of such redundant system boils down to constructing convolutional codes with good free distance over an alphabet which is in general not binary. With this respect, strongly-MDS convolutional codes constructed in this paper are particularly suited and may have potential for such applications.

Our technique of constructing MDS convolutional codes relies on the idea proposed by Aly, Grassl, Klappenecker, Rötteler and Sarvepalli [1, Theorem 3], which generalized the famous method of Piret [18] and provided a powerful machinery to construct convolutional codes from linear block codes. While this method has been employed multiple times by various authors ([2],[5]–[7],[24],[25]) to obtain some new classical and quantum MDS convolutional codes, the MDS convolutional codes obtained in these works usually have degree not larger than 2. Our contribution in this paper is the realization that by carefully adopting this method [1, Theorem 3], coupled with cyclic codes of general type [16], we can construct unit-memory MDS convolutional codes with fairly large degree.

Let us now give the structure of the paper. In Section II we review the basic theories of cyclic codes of general type and convolutional codes, in particular “strongly-MDS” convolutional codes, column distances and [1, Theorem 3], all of which will turn out to be useful in the paper. As for the construction of unit-memory MDS convolutional codes $(n, k, \delta)_q$, we treat the case $n \leq q - 1$ in Section III, the case $n = q$ in Section IV, and the case $n = q + 1$ in Section V. In Section VI we provide several explicit examples of MDS convolutional codes over the field \mathbb{F}_8 . In Section VII we conclude the paper.

II. PRELIMINARIES

In this section we review some basic theories of cyclic codes of general type and convolutional codes.

A. Cyclic codes of general type

Throughout the paper we fix some standard notation.

Let \mathbb{F}_q be the finite field of order q , where q is any prime power. An $[n, k, d]_q$ code is a k -dimensional subspace of \mathbb{F}_q^n over \mathbb{F}_q with minimum Hamming distance d . The well-known Singleton bound of an $[n, k, d]_q$ code is $d \leq n - k + 1$. If the inequality is achieved, it is called a maximal-distance-separable (MDS) code.

Definition 1. Let $0 \neq f(x) \in \mathbb{F}_q[x]$ be a monic polynomial. A nonzero ideal \mathcal{C} of the principal ideal ring $\mathbb{F}_q[x]/(f(x))$ is called a cyclic code of type f , or an f -cyclic code for short.

The concept of f -cyclic codes naturally generalizes the concept of cyclic, negacyclic and constacyclic codes, which have proved quite useful in many recent works. The basic theory of f -cyclic codes is very similar to that of cyclic, negacyclic and constacyclic codes as well and hence must have been known for a long time. In particular, for any f -cyclic code \mathcal{C} , there is

a unique monic polynomial $g \in \mathbb{F}_q[x]$ of least degree such that $g(x)|f(x)$ and $\mathcal{C} = (g(x))$. This $g(x)$ is called the generator polynomial of \mathcal{C} . Because of lacking proper references, f -cyclic codes was introduced in [16] where some of their properties were derived, with the sole purpose of providing more flexibility in constructing MDS block codes. We are grateful to Patrick Solé, who kindly pointed out that f -cyclic codes were called pseudo-cyclic codes and polycyclic codes in the literature which have been investigated, though the results which we collect below (see [16, Theorems 9 and 10]) may not be so easy to locate in the references.

Lemma 1. *Let $f \in \mathbb{F}_q[x]$ be a monic polynomial, $\deg f = n \geq 1$ and $f(x) \mid (x^{q-1} - 1)$. Let θ be a primitive element of \mathbb{F}_q . Let $g(x) = \prod_{i=d_1}^{d_2} (x - \alpha_i)$, where $\alpha_i = \theta^{a+bi}$, and d_1, d_2, a, b are some fixed integers. Assume that $g(x)|f(x)$. Let \mathcal{C} be an f -cyclic code over \mathbb{F}_q with generator polynomial g . If*

$$\frac{q-1}{(b, q-1)} \geq n \geq d_2 - d_1 + 1 \geq 1, \quad (2)$$

then \mathcal{C} is an $[n, n - d_2 + d_1 - 1, d_2 - d_1 + 1]_q$ MDS code.

Lemma 2. *Let $f \in \mathbb{F}_q[x]$ be a monic polynomial, $\deg f = n \geq 1$ and $f(x) \mid (x^{q^2-1} - 1)$. Let θ be a primitive element of \mathbb{F}_{q^2} . Let $g(x) = \prod_{i=d_1}^{d_2} (x - \alpha_i)$, where $\alpha_i = \theta^{a+bi}$, and d_1, d_2, a, b are some fixed integers. Assume that $g(x)|f(x)$.*

(i) *$g \in \mathbb{F}_q[x]$ if and only if for any i ($d_1 \leq i \leq d_2$), there exists a j ($d_1 \leq j \leq d_2$) such that*

$$q(a + bi) \equiv a + bj \pmod{q^2 - 1}. \quad (3)$$

(ii) *Assume that $g \in \mathbb{F}_q[x]$. Let \mathcal{C} be an f -cyclic code over \mathbb{F}_q with generator polynomial g . If*

$$\frac{q^2-1}{(b, q^2-1)} \geq n \geq d_2 - d_1 + 1 \geq 1, \quad (4)$$

then \mathcal{C} is an $[n, n - d_2 + d_1 - 1, d_2 - d_1 + 2]_q$ MDS code.

B. Convolutional codes

In this section we first introduce the concept of “strongly-MDS” convolutional codes, which was proposed and studied in the beautiful paper [8]. We follow the presentation of [8]. For basic theories of convolutional codes, interested readers may consult the excellent textbooks [13], [17], [18].

As in the introduction, $\mathcal{F} = \mathbb{F}_q((D))$ is the field of Laurent series over the finite field \mathbb{F}_q . Let \mathcal{C} be an $(n, k, \delta)_q$ convolutional code of memory ν , then there is a $k \times n$ minimal encoder of the form

$$G = \sum_{j=0}^{\nu} G_j D^j \in \mathbb{F}_q[D]^{k \times n}, G_j \in \mathbb{F}_q^{k \times n}, G_\nu \neq 0,$$

here ν is the memory of the code, and an $(n - k) \times n$ minimal parity-check matrix of the form

$$H = \sum_{j=0}^{\mu} H_j D^j \in \mathbb{F}_q[D]^{(n-k) \times n}, H_j \in \mathbb{F}_q^{(n-k) \times n}, H_\mu \neq 0,$$

such that

$$\mathcal{C} = \{aG : a \in \mathcal{F}^k\} = \{v \in \mathcal{F}^n : Hv^T = 0\}.$$

Both G and H are of full rank and satisfy $GH^T = 0$. The weight of $v = \sum_{j=r}^{\infty} v_j D^j \in \mathcal{F}^n$ where $v_j \in \mathbb{F}_q^n$ is defined as

$$\text{wt}(v) := \sum_{j=r}^{\infty} \text{wt}(v_j).$$

Here $\text{wt}(v_j)$ denotes the Hamming weight of $v_j \in \mathbb{F}_q^n$. The free distance of the code $\mathcal{C} \in \mathcal{F}^n$ is defined as

$$d_{\text{free}} := \min \{\text{wt}(v) : v \in \mathcal{C}, v \neq 0\}.$$

For every $j \in \mathbb{Z}_{\geq 0}$, the truncated sliding generator matrices $G_j^c \in \mathbb{F}_q^{(j+1)k \times (j+1)n}$ and parity-check matrices $H_j^c \in \mathbb{F}_q^{(j+1)(n-k) \times (j+1)n}$ are given by

$$G_j^c := \begin{bmatrix} G_0 & G_1 & \cdots & G_j \\ & G_0 & \cdots & G_{j-1} \\ & & \ddots & \vdots \\ & & & G_0 \end{bmatrix},$$

$$H_j^c := \begin{bmatrix} H_0 & & & \\ H_1 & H_0 & & \\ \vdots & \vdots & \ddots & \\ H_j & H_{j-1} & \cdots & H_0 \end{bmatrix},$$

where we let $G_j = 0$ (resp. $H_j = 0$) whenever $j > \nu$ (resp., $j > \mu$); see also [13, pp. 110]. The j -th column distance of \mathcal{C} is given by

$$\begin{aligned} d_j^c &= \min \{ \text{wt}((u_0, \dots, u_j)G_j^c) : u_i \in \mathbb{F}_q^k, u_0 \neq 0 \} \\ &= \min \{ \text{wt}(\hat{v}) : \hat{v} = (\hat{v}_0, \dots, \hat{v}_j) \in \mathbb{F}_q^{(j+1)n} : H_j^c(\hat{v})^T = 0, \hat{v}_0 \neq 0 \}. \end{aligned}$$

The $(\nu+1)$ -tuple of the numbers $(d_0^c, d_1^c, \dots, d_\nu^c)$ is called the *distance profile* of the code [13, pp. 112]. The column distances are invariants of the code \mathcal{C} ([13, Sec. 3.1]) and satisfy

- (1). $d_0^c \leq d_1^c \leq d_2^c \leq \dots \leq \lim_{j \rightarrow \infty} d_j^c = d_{\text{free}}^c$.
- (2). $d_j^c \leq (n-k)(j+1) + 1$ for every $j \in \mathbb{Z}_{\geq 0}$ ([21, Proposition 2.2]);
- (3). If $d_j^c = (n-k)(j+1) + 1$ for some $j \in \mathbb{Z}_{\geq 0}$, then $d_i^c \leq (n-k)(i+1) + 1$ for all $i \leq j$ ([21, Corollary 2.3]);
- (4). The generalized Singleton bound: $d_{\text{free}}^c \leq (n-k)(\lfloor \delta/k \rfloor + 1) + \delta + 1$ ([21, Theorem 2.6]);
- (5). Let $M := \min \{ j \in \mathbb{Z}_{\geq 0} : d_j^c = d_{\text{free}}^c \}$, then $M \geq \lfloor \delta/k \rfloor + \lceil \delta/(n-k) \rceil$ ([21, Proposition 2.7]).

From Property (5), strongly-MDS convolutional codes are MDS convolutional codes such that the generalized Singleton bound is attained by the earliest column distance possible, that is ([21, Definition 2.8]):

Definition 2. An $(n, k, \delta)_q$ code with column distance $d_j^c, j \in \mathbb{Z}_{\geq 0}$, is called *strongly-MDS*, if

$$d_M^c = (n-k)(\lfloor \delta/k \rfloor + 1) + \delta + 1, \text{ for } M = \lfloor \delta/k \rfloor + \lceil \delta/(n-k) \rceil. \quad (5)$$

The concept of “maximal distance profile” was defined in [8] and is related to the notion of optimum distance profile (ODP), see [13, pp. 112].

Definition 3. An $(n, k, \delta)_q$ code with column distance $d_j^c, j \in \mathbb{Z}_{\geq 0}$, is said to have a *maximal distance profile*, if

$$d_L^c = (n-k)(L+1) + 1, \text{ where } L = \lfloor \delta/k \rfloor + \lfloor \delta/(n-k) \rfloor. \quad (6)$$

It was proved that an $(n, k, \delta)_q$ code \mathcal{C} has a maximum distance profile if and only if the dual code \mathcal{C}^\perp has this property [8, Theorem 5.2].

Next we recall [1, Theorem 3] which provides a most powerful machinery to construct convolutional codes from linear block codes. For the sake of clarity and simplicity, we only quote the parts of [1, Theorem 3] which are most relevant to this paper. The statement of the theorem is written in slightly different form. Interested readers shall consult the original paper for details.

Theorem 2. Let \mathcal{C} be an $[n, k, d]_q$ linear code with parity check matrix $H \in \mathbb{F}_q^{(n-k) \times n}$ where $1 \leq k \leq n-2$. Assume that H is partitioned into submatrices H_0, H_1, \dots, H_m as $H^T = [H_0^T, H_1^T, \dots, H_m^T]$ such that $\kappa = \text{rank} H_0$ and $\text{rank} H_i \leq \kappa$ for $1 \leq i \leq m$ and $\kappa \geq \text{rank} H_m > 0$. Define the polynomial matrix $G(D)$ as

$$G(D) = \tilde{H}_0 + \tilde{H}_1 D + \dots + \tilde{H}_m D^m \in \mathbb{F}_q[D]^{\kappa \times n},$$

where the matrices \tilde{H}_i are obtained from H_i by adding some zero-rows so that the \tilde{H}_i all have κ rows in total. Then

- (a) The matrix $G(D)$ is a $\kappa \times n$ minimal encoder.
- (b) Let V be the convolutional code with $G(D)$ as the parity-check matrix, that is, $V = \{v \in \mathcal{F}^n : G(D)v^T = 0\}$. Let d_{free} be the free distance of V . Then

$$\min \{d_0 + d_m, d\} \leq d_{\text{free}} \leq d,$$

where d_i is the minimum distance of the code $\mathcal{C}_i := \{v \in \mathbb{F}_q^n : H_i v^T = 0\}$.

The following lemma which is a direct consequence of Theorem 2, provides guidance as to how to construct unit-memory MDS convolutional codes.

Lemma 3. Let \mathcal{C} be an $[n, k, n-k+1]_q$ MDS linear code with parity check matrix $H \in \mathbb{F}_q^{(n-k) \times n}$ where $1 \leq k \leq n-2$. Assume that H is partitioned into two submatrices H_0, H_1 as $H = \begin{bmatrix} H_0 \\ H_1 \end{bmatrix}$ such that $\gamma = \text{rank} H_0 \geq \delta = \text{rank} H_1 > 0$. Define

$$G(D) = \tilde{H}_0 + \tilde{H}_1 D,$$

where $\tilde{H}_0 = H_0$ and \tilde{H}_1 is obtained from H_1 by adding some zero-rows so that \tilde{H}_1 has γ rows in total. Then

- (a) The matrix $G(D)$ is a $\gamma \times n$ minimal encoder.
- (b) The convolutional code V obtained from $G(D)$ as a parity-check matrix has parameters $(n, k + \delta, \delta)_q$.
- (c) Let \mathcal{C}_i be the linear code with parity-check matrix $H_i, i = 0, 1$. If both \mathcal{C}_i are MDS codes, then V is a unit-memory MDS convolutional code.

Proof: Since $G(D)$ is a minimal encoder, the dual code of V has parameters $(n, \gamma, \delta)_q$, hence V has parameters $(n, n - \gamma, \delta)_q = (n, k + \delta, \delta)_q$ ([13, Theorem 2.66]). If both \mathcal{C}_i are MDS, then $d_0 \geq \gamma + 1, d_1 \geq \delta + 1$, hence $d_0 + d_1 \geq n - k + 1$ and we obtain $d_{\text{free}} = n - k + 1$ from Theorem 2. By the generalized Singleton bound (1), V is an MDS convolutional code. It is easy to see that V is of unit-memory. ■

The next lemma, adopted from [20, Theorem 28], indicates how to obtain new MDS convolutional codes from old ones.

Lemma 4. Let \mathcal{C} be an MDS $(n, k, \delta)_q$ convolutional code with minimal encoder $G(D) \in \mathbb{F}_q[D]^{k \times n}$ and row indices $v = v_1 = \dots = v_l < v_{l+1} = \dots = v_k = v + 1$. Let $\overline{G}(D) \in \mathbb{F}_q[D]^{(k-1) \times n}$ be the matrix obtained from $G(D)$ by omitting any of the last $k - l$ rows of $G(D)$, and let $\overline{\mathcal{C}}$ be the convolutional code generated by the encoder $\overline{G}(D)$. Then $\overline{\mathcal{C}}$ is also an MDS convolutional code.

III. UNIT-MEMORY MDS $(n, k, \delta)_q$ CODES WITH $n \leq q - 1$

Let $q \geq 3$ be a prime power. For any given positive integers n and k such that $k < n \leq q - 1$, define

$$f(x) = \prod_{i=0}^{n-1} (x - \theta^i), \quad g(x) = \prod_{i=0}^{n-k-1} (x - \theta^i),$$

where θ is a primitive element of \mathbb{F}_q . Let \mathcal{C} be an f -cyclic code with generator polynomial $g(x)$, that is, $\mathcal{C} = (g(x)) \subset \mathbb{F}_q[x]/(f(x))$. Then each $v(x) = \sum_{i=0}^{n-1} v_i x^i \in \mathcal{C}$ if and only if $g(x)|v(x)$, that is,

$$v(\theta^j) = 0, \quad \text{for } \forall 0 \leq j \leq n - k - 1. \quad (7)$$

By Lemma 1, \mathcal{C} is an $[n, k, n - k + 1]_q$ MDS linear code. Define the $(n - k) \times n$ matrix H by

$$H^T = [\underline{h}_0^T, \underline{h}_1^T, \dots, \underline{h}_{n-k-1}^T],$$

where each \underline{h}_j is a $1 \times n$ row-vector with entries in \mathbb{F}_q given by

$$\underline{h}_j = [1, \theta^j, \theta^{2j}, \dots, \theta^{(n-1)j}].$$

It is easy to see that the condition (7) is equivalent to $Hv^T = 0$, where $v = (v_0, v_1, \dots, v_{n-1}) \in \mathbb{F}_q^n$. Therefore H is a parity-check matrix of \mathcal{C} .

Let γ, δ be any positive integers such that $\gamma \geq \delta$ and $\gamma + \delta = n - k$. Split the matrix H into 2 disjoint submatrices H_0 and H_1 such that $H = \begin{bmatrix} H_0 \\ H_1 \end{bmatrix}$ where

$$H_0^T = [\underline{h}_0^T, \underline{h}_1^T, \dots, \underline{h}_{\gamma-1}^T], \quad H_1^T = [\underline{h}_\gamma^T, \underline{h}_{\gamma+1}^T, \dots, \underline{h}_{\gamma+\delta-1}^T].$$

It shall be noted that any γ columns of H_0 (resp. any δ columns of H_1) are linearly independent, so let \mathcal{C}_i be the linear code over \mathbb{F}_q by the parity-check matrix $H_i, i = 0, 1$, then each \mathcal{C}_i is an MDS code.

Define two $\gamma \times n$ matrices \tilde{H}_0, \tilde{H}_1 by

$$\tilde{H}_0 = H_0, \quad \tilde{H}_1^T = [\mathbf{0}_{n \times (\gamma - \delta)}, \underline{h}_\gamma^T, \underline{h}_{\gamma+1}^T, \dots, \underline{h}_{\gamma+\delta-1}^T].$$

Here $\mathbf{0}_{r \times s}$ denotes the $r \times s$ zero matrix for any positive integers r and s . Let $V \in \mathcal{F}^n$ be the convolutional code defined by the parity-check matrix $G(D)$ given by

$$g(D) = \tilde{H}_0 + \tilde{H}_1 D.$$

We prove the following result.

Theorem 3. (i). The code V defined above is an $(n, k + \delta, \delta)_q$ unit-memory MDS convolutional code whenever

$$1 \leq k < n \leq q - 1, \quad 1 \leq \delta \leq \frac{n - k}{2}.$$

(ii). The code V is an $(n, k + \delta, \delta)_q$ unit-memory MDS convolutional code with a maximal distance profile whenever

$$1 \leq k < n \leq q - 1, \quad 1 \leq \delta < \frac{n - k}{2}.$$

(iii). The code V defined above is an $(n, k + \delta, \delta)_q$ unit-memory strongly-MDS convolutional code whenever

$$1 \leq k < n \leq q - 1, \quad 1 \leq \delta \leq \frac{n - k + 1}{3}.$$

Proof: (i) follows directly from Lemma 3, as $\mathcal{C}_0, \mathcal{C}_1$ are both MDS linear codes.

(ii) is obvious since $L = \lfloor \delta/(k + \delta) \rfloor + \lfloor \delta/(n - k - \delta) \rfloor = 0$.

As for (iii), since $M = \lfloor \delta/(k + \delta) \rfloor + \lceil \delta/(n - k - \delta) \rceil = 1$ and $d_1^c \leq d_{\text{free}} = d = n - k + 1$, it suffices to prove that

$$d_1^c \geq d = n - k + 1, \quad (8)$$

where d_1^c is the 1-st column distance of \mathcal{C} which is given by

$$d_1^c = \min \left\{ \text{wt}(\hat{v}) : \hat{v} = (\hat{v}_0, \hat{v}_1) \in \mathbb{F}_q^{2n} : H_1^c(\hat{v})^T = 0, \hat{v}_0 \neq 0 \right\},$$

and the matrix H_1^c is given by

$$H_1^c := \begin{bmatrix} H_0 & 0 \\ \tilde{H}_1 & H_0 \end{bmatrix}.$$

For $v = (v_0, v_1)$ where $v_0, v_1 \in \mathbb{F}_q^n$ and $v_0 \neq 0$ such that $H_1^c v^T = 0$, that is, $H_0 v_0^T = 0$ and $\tilde{H}_1 v_0^T + H_0 v_1^T = 0$. If $v_1 = 0$, then $H v_0^T = 0$, thus $0 \neq v_0 \in \mathcal{C}$ and $\text{wt}(v_0) \geq d = n - k + 1$. If $v_1 \neq 0$, we have $v_0 \in \mathcal{C}_0$ and $\text{wt}(v_0) \geq d_0 = \gamma + 1$. Noting that $\gamma - \delta \geq \delta - 1$, the equation $\tilde{H}_1 v_0^T + H_0 v_1^T = 0$ implies that $\Gamma v_1^T = 0, v_1 \neq 0$ where

$$\Gamma^T = [\underline{h}_0^T, \underline{h}_1^T, \dots, \underline{h}_{\gamma-\delta-1}^T].$$

It is easy to see that any $\gamma - \delta$ columns of Γ are linearly independent. This implies that $\text{wt}(v_1) \geq \gamma - \delta + 1 \geq \delta$, hence we have $\text{wt}(v) = \text{wt}(v_0) + \text{wt}(v_1) \geq \gamma + 1 + \delta = n - k + 1$. This confirms (8) and completes the proof of (iii). ■

We remark that (i) of Theorem 3 can be proved by using the generalized Reed-Solomon (\mathcal{GRS}) code as well.

IV. UNIT-MEMORY MDS $(q, k, \delta)_q$ CODES

Again let $q \geq 3$ be a prime power. For $n = q$ we find it is most convenient to use the generalized Reed-Solomon (\mathcal{GRS}) codes of length q to construct unit-memory $(q, k, \delta)_q$ codes, though it is quite possible that f -cyclic codes may be used for this purpose as well.

Let θ be a primitive element of \mathbb{F}_q . Let $\mathbf{v} = (0, \theta, \dots, \theta^{q-1})$ and $\mathbf{w} = (w_0, w_1, \dots, w_{q-1})$ where $w_i \in \mathbb{F}_q^*$ for each i . For any positive integer $k < q$, the \mathcal{GRS} code $\mathcal{C} = \mathcal{GRS}_k(\mathbf{v}, \mathbf{w})$ is defined by

$$\mathcal{GRS}_k(\mathbf{v}, \mathbf{w}) = \left\{ (w_0 f(0), w_1 f(\theta), \dots, w_{q-1} f(\theta^{q-1})) : f \in \mathcal{P}_k \right\},$$

where $\mathcal{P}_k \subset \mathbb{F}_q[x]$ is the set of polynomials of degree less than k . It is known that \mathcal{C} is an $[q, k, q - k + 1]_q$ MDS linear code and a parity check matrix of \mathcal{C} is given by

$$H = \begin{bmatrix} u_0 & u_1 & u_2 & \cdots & u_{q-1} \\ 0 & u_1 \theta & u_2 \theta^2 & \cdots & u_{q-1} \theta^{q-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & u_1 \theta^{q-k-1} & u_2 \theta^{2(q-k-1)} & \cdots & u_{q-1} \theta^{(q-1)(q-k-1)} \end{bmatrix}_{(q-k) \times q},$$

where $u_i \in \mathbb{F}_q^*$ can be determined by \mathcal{C} (see [12, Theorem 5.3.3]). Let \underline{h}_j be the $j + 1$ -th row of H . For any positive integers γ, δ such that $\gamma \geq \delta$ and $\gamma + \delta = q - k$, we split the matrix H into 2 disjoint submatrices H_0 and H_1 such that $H = \begin{bmatrix} H_0 \\ H_1 \end{bmatrix}$ where

$$H_0^T = [\underline{h}_0^T, \underline{h}_1^T, \dots, \underline{h}_{\gamma-1}^T], \quad H_1^T = [\underline{h}_{\gamma+\delta-1}^T, \underline{h}_{\gamma+\delta-2}^T, \dots, \underline{h}_{\gamma}^T].$$

Define two $\gamma \times q$ matrices \tilde{H}_0, \tilde{H}_1 by

$$\tilde{H}_0 = H_0, \quad \tilde{H}_1^T = [\mathbf{0}_{\gamma \times (\gamma-\delta)}, \underline{h}_{\gamma+\delta-1}^T, \underline{h}_{\gamma+\delta-2}^T, \dots, \underline{h}_{\gamma}^T].$$

Let $V \in \mathcal{F}^n$ be the convolutional code defined by the parity-check matrix $G(D)$ given by

$$g(D) = \tilde{H}_0 + \tilde{H}_1 D.$$

We prove the following result.

Theorem 4. (i). The code V defined above is an $(q, k + \delta, \delta)_q$ unit-memory MDS convolutional code whenever

$$1 \leq k < q, \quad 1 \leq \delta \leq \frac{q - k}{2}.$$

(ii). The code V is an $(q, k + \delta, \delta)_q$ unit-memory MDS convolutional code with a maximal distance profile whenever

$$1 \leq k < q, \quad 1 \leq \delta < \frac{q-k}{2}.$$

(iii). The code V defined above is an $(q, k + \delta, \delta)_q$ unit-memory strongly-MDS convolutional code whenever

$$1 \leq k < q, \quad 1 \leq \delta \leq \frac{q-k+1}{3}.$$

Proof: It is clear that V is an $(q, k + \delta, \delta)_q$ code. The arguments of (ii) and (iii) are exactly the same as those of (ii) and (iii) of Theorem 3 respectively, hence we omit details. We only prove (i), the proof of which is quite different from that of (i) in Theorem 3.

To prove (i), it suffices to prove that there exists a sufficiently large integer j such that the j -th column distance d_j^c of \mathcal{C} satisfies $d_j^c \geq n - k + 1 = \gamma + \delta + 1$, since $d_{\text{free}} \geq d_j^c$ for any j . Here

$$d_j^c = \min \left\{ \text{wt}(\hat{v}) : \hat{v} = (\hat{v}_0, \dots, \hat{v}_j) \in \mathbb{F}_q^{(j+1)n} : H_j^c(\hat{v})^T = 0, \hat{v}_0 \neq 0 \right\},$$

where

$$H_j^c = \begin{bmatrix} H_0 & & & & & \\ \tilde{H}_1 & H_0 & & & & \\ & \tilde{H}_1 & H_0 & & & \\ & & & \ddots & \ddots & \\ & & & & \tilde{H}_1 & H_0 \end{bmatrix}.$$

For any $v_i \in \mathbb{F}_q^n$, $0 \leq i \leq j$ and $v_0 \neq 0$, for the sake of convenience we write each v_i as a column vector. Let $v^T = (v_0^T, \dots, v_j^T)$ and suppose $H_j^c v = 0$. This is equivalent to $H_0 v_0 = 0$ and $\tilde{H}_1 v_{i-1} + H_0 v_i = 0$ for each $1 \leq i \leq j$. Let \mathcal{C}_0 be the linear code defined by the parity-check matrix H_0 . Obviously \mathcal{C}_0 is a $[q, q - \gamma, \gamma + 1]_q$ MDS code and $0 \neq v_0 \in \mathcal{C}_0$, hence $\text{wt}(v_0) \geq \gamma + 1$. Our goal is to prove $\text{wt}(v) \geq \gamma + \delta + 1$ when j is sufficiently large. The argument is dividend into several cases, which we will describe as below.

Case 1. If $\#\{1 \leq i \leq j : v_i \neq 0\} \geq \delta$, then $\text{wt}(v) = \sum_i \text{wt}(v_i) \geq \gamma + \delta + 1$, done.

Case 2. If $\#\{1 \leq i \leq j : v_i \neq 0\} = 0$, that is, $v_1 = \dots = v_j = 0$, then $Hv_0 = 0$, hence $v_0 \in \mathcal{C}$ and $\text{wt}(v_0) \geq d = \gamma + \delta + 1$, done.

Case 3. If there is some i such that $v_i = 0$ but $v_{i+1} \neq 0$, then from $\tilde{H}_1 v_i + H_0 v_{i+1} = H_0 v_{i+1} = 0$ we have $0 \neq v_{i+1} \in \mathcal{C}_0$ with $\text{wt}(v_{i+1}) \geq \gamma + 1$, thus $\text{wt}(v) \geq \text{wt}(v_0) + \text{wt}(v_{i+1}) \geq 2\gamma + 2 \geq \gamma + \delta + 1$, done.

It remains to consider the case that there is an integer i in the range $1 \leq i < \delta$ such that $v_t \neq 0$ for any $t \leq i$ and $v_t = 0$ for any $t > i$. The equations are $\tilde{H}_1 v_i + H_0 v_{i+1} = \tilde{H}_1 v_i = 0$ and $\tilde{H}_1 v_{i-1} + H_0 v_i = 0$.

Case 4. If $\text{wt}(v_i) \geq 2$, from $H_1 v_i = 0$ and the definition of H_1 we see that $\text{wt}(v_i) \geq \delta + 1$, done.

Case 5. Now suppose $\text{wt}(v_i) = 1$. Then v_i must be of the form $v_i^T = (\alpha, 0, \dots, 0)$ for some $\alpha \in \mathbb{F}_q^*$. If $\gamma > \delta$, then it is impossible to have $\tilde{H}_1 v_{i-1} + H_0 v_i = 0$. So we shall assume that $\gamma = \delta$. Thus $\tilde{H}_1 = H_1$. We may assume that $\gamma = \delta \geq 2$, because if otherwise then $\text{wt}(v) \geq \text{wt}(v_0) + \text{wt}(v_i) \geq \gamma + \delta + 1$ is trivial.

Case 5 i). If $i \geq 2$, from $H_1 v_{i-1} + H_0 v_i = H_1 v_{i-1} + [\alpha, 0, \dots, 0]^T = 0$ and the definition of H_1 we obtain $\Gamma v_{i-1} = 0$ where $\Gamma^T = [\underline{h}_{\gamma+\delta-2}^T, \underline{h}_{\gamma+\delta-3}^T, \dots, \underline{h}_\gamma^T]$. If $\text{wt}(v_{i-1}) \geq 2$, then $\text{wt}(v_{i-1}) \geq \delta$, thus $\text{wt}(v) \geq \text{wt}(v_0) + \text{wt}(v_{i-1}) + \text{wt}(v_i) \geq \gamma + \delta + 1$, done. If $\text{wt}(v_{i-1}) = 1$, then v_{i-1} must be of the form $v_{i-1}^T = (\beta, 0, \dots, 0)$ for some $\beta \in \mathbb{F}_q^*$. However this contradicts to the equation $H_1 v_{i-1} + H_0 v_i = 0$.

Case 5 ii). Finally we consider that case that $i = 1$, that is, $v_0 \neq 0, v_1 \neq 0, v_t = 0$ for any $t \geq 2$. The equations $H_0 v_0 = 0$ and $\tilde{H}_1 v_0 + H_0 v_1 = 0$ where $v_1^T = (\alpha, 0, \dots, 0), \alpha \in \mathbb{F}_q^*$ implies that $\tilde{\Gamma} \hat{v}_0 = 0$ where $\tilde{\Gamma} = [\underline{h}_0, \dots, \underline{h}_{\gamma+\delta-2}]$, where \hat{v}_0 is a rearrangement of entries of v_0 and hence they have the same Hamming weight. Thus $\text{wt}(v_0) \geq \gamma + \delta$ and therefore $\text{wt}(v) = \text{wt}(v_0) + \text{wt}(v_1) \geq \gamma + \delta + 1$, done.

We conclude that in all cases we have $\text{wt}(v) \geq \gamma + \delta + 1$. This proves $d_j^c \geq \gamma + \delta + 1$ for some j , and the proof of (i) is now complete. ■

V. UNIT-MEMORY MDS $(q + 1, k, \delta)_q$ CODES

Let θ be a primitive element of \mathbb{F}_{q^2} and $\beta := \theta^{q-1}$. Then β is a primitive $(q + 1)$ -th root of unity in \mathbb{F}_{q^2} and $\beta^q = \beta^{-1}$. Let k be any positive integer k such that $1 \leq k < q + 1$. We first consider the case that $k \equiv q \pmod{2}$.

A. Part 1. $k \equiv q \pmod{2}$

Define $\tau := \frac{q-k}{2}$ and

$$g(x) = \prod_{j=-\tau}^{\tau} (x - \beta^j).$$

It is clear that $\deg g = 2\tau + 1$, $g(x) \in \mathbb{F}_q[x]$ and $g(x) \mid (x^{q+1} - 1)$. Let $\mathcal{C} = (g(x)) \subset \mathbb{F}_q[x]/(x^{q+1} - 1)$ be the cyclic code of length $q + 1$ with generator polynomial $g(x)$. It is known from Lemma 2 that \mathcal{C} is a $[q + 1, k, 2\tau + 2]_q$ MDS code.

Each $v(x) = \sum_{i=0}^q v_i x^i \in \mathcal{C}$ if and only if $g(x) \mid v(x)$, that is,

$$v(\beta^j) = 0, \quad \text{for } \forall -\tau \leq j \leq \tau. \quad (9)$$

Because $v_i \in \mathbb{F}_q$ and $\beta^q = \beta^{-1}$, this is equivalent to

$$v(\beta^j) = 0, \quad \text{for } \forall 0 \leq j \leq \tau. \quad (10)$$

Denote for each j

$$\underline{h}_j = [1, \beta^j, \beta^{2j}, \dots, \beta^{qj}],$$

and define

$$\begin{aligned} \overline{H}^T &= [\underline{h}_{-\tau}^T, \dots, \underline{h}_{-1}^T, \underline{h}_0^T, \underline{h}_1^T, \dots, \underline{h}_\tau^T], \\ H^T &= [\underline{h}_0^T, \underline{h}_1^T, \dots, \underline{h}_\tau^T]. \end{aligned} \quad (11)$$

(9) and (10) imply that for any $v = (v_0, \dots, v_q) \in \mathcal{C} \subset \mathbb{F}_q^{q+1}$ if and only if $\overline{H}v^T = 0$ if and only if $Hv^T = 0$.

Each vector \underline{h}_j ($1 \leq j \leq \tau$) which is originally defined over \mathbb{F}_{q^2} can be identified with two rows of length $q + 1$ defined over \mathbb{F}_q . More precisely, let $\{1, e\}$ be a basis of \mathbb{F}_{q^2} over \mathbb{F}_q , then $\underline{h}_j = \underline{h}_{j,1} + e\underline{h}_{j,2}$ where $\underline{h}_{j,i}$, $i = 1, 2$ are defined over \mathbb{F}_q . We identify \underline{h}_j with $\begin{bmatrix} \underline{h}_{j,1} \\ \underline{h}_{j,2} \end{bmatrix}$, which is a $2 \times (q + 1)$ matrix over \mathbb{F}_q . Under this identification H becomes a $(2\tau + 1) \times (q + 1)$ matrix over \mathbb{F}_q , and $v = (v_0, \dots, v_q) \in \mathcal{C}$ if and only if $Hv^T = 0$, hence H can be regarded as a parity-check matrix of \mathcal{C} . In what follows each \underline{h}_j , $j \geq 1$ shall be thought of as either one row over \mathbb{F}_{q^2} or equivalently two rows over \mathbb{F}_q .

To construct convolutional codes from H , we split the matrix H into 2 disjoint submatrices H_0 and H_1 such that $H = \begin{bmatrix} H_0 \\ H_1 \end{bmatrix}$. There are two different ways to do that.

Construction one. Let $q \geq 5$. For any positive integers γ, δ such that $\gamma > \delta$ and $\gamma + \delta = \tau + 1$, define H_0, H_1 as

$$H_0^T = [\underline{h}_0^T, \underline{h}_1^T, \dots, \underline{h}_{\gamma-1}^T], \quad H_1^T = [\underline{h}_\gamma^T, \underline{h}_{\gamma+1}^T, \dots, \underline{h}_{\gamma+\delta-1}^T].$$

Considered as matrices over \mathbb{F}_q , H_0, H_1 are of size $(2\gamma - 1) \times (q + 1)$ and $2\delta \times (q + 1)$ respectively. It shall be noted that any $(2\gamma - 1)$ columns of H_0 are linearly independent, because for any $v = (v_1, \dots, v_q) \in \mathbb{F}_q^{q+1}$, $H_0 v^T = 0$ if and only if $\overline{H}_0 v^T = 0$ where

$$\overline{H}_0^T = [\underline{h}_{-(\gamma-1)}^T, \dots, \underline{h}_{-1}^T, \underline{h}_0^T, \underline{h}_1^T, \dots, \underline{h}_{\gamma-1}^T].$$

Define two $(2\gamma - 1) \times (q + 1)$ matrices \tilde{H}_0, \tilde{H}_1 by

$$\tilde{H}_0 = H_0, \quad \tilde{H}_1^T = [\mathbf{0}_{(q+1) \times (2\gamma-1-2\delta)}, \underline{h}_\gamma^T, \underline{h}_{\gamma+1}^T, \dots, \underline{h}_{\gamma+\delta-1}^T].$$

Let $V \in \mathcal{F}^{q+1}$ be the convolutional code defined by the parity-check matrix $G(D)$ given by

$$g(D) = \tilde{H}_0 + \tilde{H}_1 D.$$

We prove the following result.

Theorem 5. *The code V defined above is a $(q + 1, k + 2\delta, 2\delta)_q$ unit-memory strongly-MDS convolutional code whenever*

$$k \equiv q \pmod{2}, \quad 1 \leq k < q, \quad 1 \leq \delta \leq \frac{q - k + 2}{6}.$$

In this case V also has a maximal distance profile.

Proof: First it is clear that V is an $(q + 1, k + 2\delta, 2\delta)_q$ convolutional code.

Since $M = \lfloor 2\delta/(k + 2\delta) \rfloor + \lceil 2\delta/(q + 1 - k - 2\delta) \rceil = 1$ and $d_1^c \leq d_{\text{free}} \leq d = q + 2 - k$ by the generalized Singleton bound (1), it suffices to prove that

$$d_1^c \geq d = q + 2 - k, \quad (12)$$

where d_1^c is the 1-st column distance of \mathcal{C} which is given by

$$d_1^c = \min \left\{ \text{wt}(\hat{v}) : \hat{v} = (\hat{v}_0, \hat{v}_1) \in \mathbb{F}_q^{2(q+1)} : H_1^c(\hat{v})^T = 0, \hat{v}_0 \neq 0 \right\}.$$

The matrix H_1^c is given by

$$H_1^c := \begin{bmatrix} H_0 & 0 \\ \tilde{H}_1 & H_0 \end{bmatrix}.$$

For $v = (v_0, v_1)$ where $v_0, v_1 \in \mathbb{F}_q^{q+1}$ and $v_0 \neq 0$ such that $H_1^c v^T = 0$, that is, $H_0 v_0^T = 0$ and $\tilde{H}_1 v_0^T + H_0 v_1^T = 0$. If $v_1 = 0$, then $H v_0^T = 0$, thus $0 \neq v_0 \in \mathcal{C}$ and $\text{wt}(v_0) \geq d = q + 2 - k$. If $v_1 \neq 0$, we have $v_0 \in \mathcal{C}_0$ and $\text{wt}(v_0) \geq d_0 = 2\gamma$. Noting that $\gamma > \delta$, the equation $\tilde{H}_1 v_0^T + H_0 v_1^T = 0$ implies that $\Gamma v_1^T = 0$ where

$$\Gamma^T = [\underline{h}_0^T, \underline{h}_1^T, \dots, \underline{h}_{\gamma-\delta-1}^T].$$

Define

$$\bar{\Gamma}^T = [\underline{h}_{-(\gamma-\delta-1)}^T, \dots, \underline{h}_0^T, \underline{h}_1^T, \dots, \underline{h}_{\gamma-\delta-1}^T].$$

It is easy to see that $\Gamma v_1^T = 0$ if and only if $\bar{\Gamma} v_1^T = 0$, since $v_1 \neq 0$, it implies that $\text{wt}(v_1) \geq 2(\gamma - \delta) \geq 2\delta$, hence we still have $\text{wt}(v) = \text{wt}(v_0) + \text{wt}(v_1) \geq 2\gamma + 2\delta = q + 2 - k$. This confirms (12) and completes the proof of Theorem 5. ■

Construction two. We assume that $q \geq 4$ is even. Let H_e be the submatrix of H which consists of the \underline{h}_j for all even j where $0 \leq j \leq \tau$, and let H_o be the submatrix of H which consists of the \underline{h}_j for all odd j where $0 \leq j \leq \tau$. Let r and s the number of even j 's and the number of odd j 's respectively in the range $0 \leq j \leq \tau$. Then $r + s = \tau + 1$. Let \mathcal{C}_o and \mathcal{C}_e be the linear codes obtained by H_o, H_e as parity-check matrices respectively. It is easy to see that both $\mathcal{C}_o, \mathcal{C}_e$ are MDS linear codes when q is even (see Lemma 2). This is because, for example, for any $v = (v_0, \dots, v_q) \in \mathbb{F}_q^{q+1}$, $H_e v^T = 0$ if and only if $\bar{H}_e v^T = 0$ where \bar{H}_e is given by

$$\bar{H}_e^T = [\dots, \underline{h}_{-2}^T, \underline{h}_0^T, \underline{h}_2^T, \dots].$$

Now it is clear that any $2r - 1$ columns of H_e are linearly independent. This argument also applies to H_o .

We consider H_e, H_o as matrices over \mathbb{F}_q . If $2r - 1 > 2s$, define $\tilde{H}_0 = H_e$ and define \tilde{H}_1 to be the matrix obtained from H_o by adding zero rows; if $2r - 1 < 2s$, define $\tilde{H}_0 = H_o$ and define \tilde{H}_1 to be the matrix obtained from H_e by adding zero rows. Define

$$G(D) = \tilde{H}_0 + \tilde{H}_1 D,$$

and let $V \in \mathcal{F}^{q+1}$ be the convolutional code defined by the parity-check matrix $G(D)$. We have the following result.

Theorem 6. *If $q \geq 4$ is even, the code V defined above is a $(q + 1, q - \tau, \tau)_q$ MDS convolutional code for any τ such that*

$$1 \leq \tau \leq \frac{q-1}{2}.$$

Proof: Lemma 3 implies directly that V is an MDS convolutional code of length $q + 1$. As for other parameters of V , if τ is even, then $r = \frac{\tau}{2} + 1, s = \frac{\tau}{2}$, and $2r - 1 > 2s$, then V has degree $2s = \tau$ and dimension $q + 1 - (2r - 1) = q - \tau$. If τ is odd, then $r = s = \frac{\tau+1}{2}$, $2r - 1 < 2s$, hence V has degree $2r - 1 = \tau$ and dimension $q + 1 - 2s = q - \tau$. This concludes the proof of Theorem 6. ■

B. Part 2. $k \equiv q + 1 \pmod{2}$

Again let $q \geq 5$. Define $\tau := \frac{q-k-1}{2}$ and

$$g(x) = \prod_{j=-\tau}^{\tau+1} (x - \theta\beta^j).$$

It is clear that $\deg g = 2\tau + 2 = q + 1 - k$, $g(x) \in \mathbb{F}_q[x]$ and $g(x) \mid (x^{q+1} - \theta^{q+1})$. Let $\mathcal{C} = (g(x)) \subset \mathbb{F}_q[x] / (x^{q+1} - \theta^{q+1})$ be the constacyclic code of length $q + 1$ with generator polynomial $g(x)$. It is known from Lemma 2 that \mathcal{C} is a $[q + 1, k, 2\tau + 3]_q$ MDS code.

Each $v(x) = \sum_{i=0}^q v_i x^i \in \mathcal{C}$ if and only if $g(x) \mid v(x)$, that is,

$$v(\theta\beta^j) = 0, \quad \text{for } \forall -\tau \leq j \leq \tau + 1. \quad (13)$$

Because $v_i \in \mathbb{F}_q$ and $(\theta\beta^j)^q = \theta\beta^{1-j}$, this is equivalent to

$$v(\theta\beta^j) = 0, \quad \text{for } \forall 1 \leq j \leq \tau + 1. \quad (14)$$

Denote for each j

$$\underline{h}_j = [1, \theta\beta^j, (\theta\beta^j)^2, \dots, (\theta\beta^j)^q],$$

and define

$$\begin{aligned}\overline{H}^T &= [\underline{h}_{-\tau}^T, \dots, \underline{h}_{-1}^T, \underline{h}_0^T, \underline{h}_1^T, \dots, \underline{h}_{\tau+1}^T], \\ H^T &= [\underline{h}_1^T, \dots, \underline{h}_{\tau+1}^T].\end{aligned}$$

(13) and (14) imply that for any $v = (v_0, \dots, v_q) \in \mathcal{C} \subset \mathbb{F}_q^{q+1}$ if and only if $\overline{H}v^T = 0$ if and only if $Hv^T = 0$.

Similar as before, we identify each \underline{h}_j ($1 \leq j \leq \tau + 1$) with $\begin{bmatrix} \underline{h}_{j,1} \\ \underline{h}_{j,2} \end{bmatrix}$, which is a $2 \times (q + 1)$ matrix over \mathbb{F}_q . Under this identification H becomes a $(2\tau + 2) \times (q + 1)$ matrix over \mathbb{F}_q , and $v = (v_0, \dots, v_q) \in \mathcal{C}$ if and only if $Hv^T = 0$, hence H can be regarded as a parity-check matrix of \mathcal{C} . In what follows each \underline{h}_j , $j \geq 1$ shall be thought of as either one row over \mathbb{F}_{q^2} or equivalently two rows over \mathbb{F}_q .

For any positive integers γ, δ such that $\gamma \geq \delta$ and $\gamma + \delta = \tau + 1$, we split the matrix H into 2 disjoint submatrices H_0 and H_1 such that $H = \begin{bmatrix} H_0 \\ H_1 \end{bmatrix}$, where H_0 and H_1 are given by

$$H_0^T = [\underline{h}_1^T, \dots, \underline{h}_\gamma^T], \quad H_1^T = [\underline{h}_{\gamma+1}^T, \underline{h}_{\gamma+2}^T, \dots, \underline{h}_{\gamma+\delta}^T].$$

Considered as matrices over \mathbb{F}_q , H_0, H_1 are of size $2\gamma \times (q + 1)$ and $2\delta \times (q + 1)$ respectively. It shall be noted that any 2γ columns of H_0 are linearly independent.

Define two $2\gamma \times (q + 1)$ matrices \tilde{H}_0, \tilde{H}_1 by

$$\tilde{H}_0 = H_0, \quad \tilde{H}_1^T = [\mathbf{0}_{(q+1) \times (2\gamma-2\delta)}, \underline{h}_{\gamma+1}^T, \underline{h}_{\gamma+2}^T, \dots, \underline{h}_{\gamma+\delta}^T].$$

Let $V \in \mathcal{F}^{q+1}$ be the convolutional code defined by the parity-check matrix $G(D)$ given by

$$g(D) = \tilde{H}_0 + \tilde{H}_1 D.$$

We prove the following result.

Theorem 7. *The code V defined above is a $(q + 1, k + 2\delta, 2\delta)_q$ unit-memory strongly-MDS convolutional code whenever*

$$k \equiv q + 1 \pmod{2}, \quad 1 \leq k < q, \quad 1 \leq \delta \leq \frac{q - k + 1}{6}.$$

In this case V also has a maximal distance profile.

Proof: The proof is very similar to that of Theorem 5. For the sake of completeness, we provide all details here.

First it is clear that V is an $(q + 1, k + 2\delta, 2\delta)_q$ convolutional code.

Since $M = \lfloor 2\delta/(k + 2\delta) \rfloor + \lceil 2\delta/(q + 1 - k - 2\delta) \rceil = 1$ and $d_1^c \leq d_{\text{free}} \leq d = q + 2 - k$ by the generalized Singleton bound, it suffices to prove that

$$d_1^c \geq d = q + 2 - k, \tag{15}$$

where d_1^c is the 1-st column distance of \mathcal{C} which is given by

$$d_1^c = \min \left\{ \text{wt}(\hat{v}) : \hat{v} = (\hat{v}_0, \hat{v}_1) \in \mathbb{F}_q^{2n} : H_1^c(\hat{v})^T = 0, \hat{v}_0 \neq 0 \right\},$$

and the matrix H_1^c is given by

$$H_1^c := \begin{bmatrix} H_0 & 0 \\ \tilde{H}_1 & H_0 \end{bmatrix}.$$

For $v = (v_0, v_1)$ where $v_0, v_1 \in \mathbb{F}_q^{q+1}$ and $v_0 \neq 0$ such that $H_1^c v^T = 0$, that is, $H_0 v_0^T = 0$ and $\tilde{H}_1 v_0^T + H_0 v_1^T = 0$. If $v_1 = 0$, then $Hv_0^T = 0$, thus $0 \neq v_0 \in \mathcal{C}$ and $\text{wt}(v_0) \geq d = q + 2 - k$. If $v_1 \neq 0$, we have $v_0 \in \mathcal{C}_0$ and $\text{wt}(v_0) \geq d_0 = 2\gamma + 1$. Noting that $\gamma > \delta$, the equation $\tilde{H}_1 v_0^T + H_0 v_1^T = 0$ implies that $\Gamma v_1^T = 0$ where

$$\Gamma^T = [\underline{h}_1^T, \dots, \underline{h}_{\gamma-\delta}^T].$$

Define

$$\overline{\Gamma}^T = [\underline{h}_{1-(\gamma-\delta)}^T, \dots, \underline{h}_0^T, \underline{h}_1^T, \dots, \underline{h}_{\gamma-\delta}^T].$$

It is easy to see that $\Gamma v_1^T = 0$ if and only if $\overline{\Gamma} v_1^T = 0$, since $v_1 \neq 0$, it implies that $\text{wt}(v_1) \geq 2(\gamma - \delta) + 1 \geq 2\delta$, hence we still have $\text{wt}(v) = \text{wt}(v_0) + \text{wt}(v_1) \geq 2\gamma + 2\delta + 1 = q + 2 - k$. This confirms (15) and completes the proof of Theorem 7. ■

VI. EXAMPLES OF MDS CONVOLUTIONAL CODES OVER \mathbb{F}_8

In this section, we present some explicit examples of MDS and strongly-MDS convolutional codes over \mathbb{F}_8 . Hence $q = 8$. Let θ be a root of the irreducible polynomial $x^3 + x + 1$ over \mathbb{F}_2 . We know that θ is a primitive element of \mathbb{F}_8 , that is, θ has order $8 - 1 = 7$. The elements of \mathbb{F}_8 are: $0, 1, \theta, \theta^2, \theta^3 = 1 + \theta, \theta^4 = \theta + \theta^2, \theta^5 = 1 + \theta + \theta^2, \theta^6 = 1 + \theta^2$. We consider the following cases:

A. Case 1: $n = q - 1 = 7$

From Theorem 3, we consider cyclic codes \mathcal{C} of length 7 over \mathbb{F}_8 , that is, $\mathcal{C} = (g(x)) \subset \mathbb{F}_8[x]/(x^7 - 1)$.

Example 1: MDS $(7, 4, 2)_8$

Here $k = 2, \delta = 2$. Consider the cyclic code \mathcal{C} of length 7 over \mathbb{F}_8 with generator polynomial $g(x) = \prod_{i=0}^4 (x - \theta^i)$. Note that $\deg g = 5$, so \mathcal{C} is a $[7, 2, 6]_8$ MDS linear code by Lemma 1.

A parity-check matrix H of \mathcal{C} is given by

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \theta & \theta^2 & \theta^3 & \theta^4 & \theta^5 & \theta^6 \\ 1 & \theta^2 & \theta^4 & \theta^6 & \theta^8 & \theta^{10} & \theta^{12} \\ 1 & \theta^3 & \theta^6 & \theta^9 & \theta^{12} & \theta^{15} & \theta^{18} \\ 1 & \theta^4 & \theta^8 & \theta^{12} & \theta^{16} & \theta^{20} & \theta^{24} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \theta & \theta^2 & 1 + \theta & \theta + \theta^2 & 1 + \theta + \theta^2 & 1 + \theta^2 \\ 1 & \theta^2 & \theta + \theta^2 & 1 + \theta^2 & \theta & 1 + \theta & 1 + \theta + \theta^2 \\ 1 & 1 + \theta & 1 + \theta^2 & \theta^2 & 1 + \theta + \theta^2 & \theta & \theta + \theta^2 \\ 1 & \theta + \theta^2 & \theta & 1 + \theta + \theta^2 & \theta^2 & 1 + \theta^2 & 1 + \theta \end{bmatrix}$$

Now let H_0 be the first $n - k - \delta = 3$ rows of H and H_1 be the rest $\delta = 2$ rows. Then consider the convolutional code V with parity-check matrix

$$G(D) = H_0 + \tilde{H}_1 D$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1+D & \theta+(1+\theta)D & \theta^2+(1+\theta^2)D & (1+\theta)+\theta^2 D & (\theta+\theta^2)+(1+\theta+\theta^2)D & (1+\theta+\theta^2)+\theta D & (1+\theta^2)+(\theta+\theta^2)D \\ 1+D & \theta^2+(\theta+\theta^2)D & (\theta+\theta^2)+\theta D & (1+\theta^2)+(1+\theta+\theta^2)D & \theta+\theta^2 D & (1+\theta)+(1+\theta^2)D & (1+\theta+\theta^2)+(1+\theta)D \end{bmatrix}$$

By Theorem 3 (i), V is a unit-memory MDS convolutional code with parameters $(7, 4, 2)_8$. The free distance of V is 6. Noting by (ii) and (iii) of Theorem 3, V has a maximal distance profile and is also strongly-MDS.

Example 2: MDS $(7, 3, 2)_8$

Here $k = 1, \delta = 2$. Consider the cyclic code \mathcal{C} of length 7 over \mathbb{F}_8 with generator polynomial $g(x) = \prod_{i=0}^5 (x - \theta^i)$. Note that $\deg g = 6$, so \mathcal{C} is a $[7, 1, 7]_8$ MDS linear code by Lemma 1.

A parity-check matrix H of \mathcal{C} is given by

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \theta & \theta^2 & \theta^3 & \theta^4 & \theta^5 & \theta^6 \\ 1 & \theta^2 & \theta^4 & \theta^6 & \theta^8 & \theta^{10} & \theta^{12} \\ 1 & \theta^3 & \theta^6 & \theta^9 & \theta^{12} & \theta^{15} & \theta^{18} \\ 1 & \theta^4 & \theta^8 & \theta^{12} & \theta^{16} & \theta^{20} & \theta^{24} \\ 1 & \theta^5 & \theta^{10} & \theta^{15} & \theta^{20} & \theta^{25} & \theta^{30} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \theta & \theta^2 & 1 + \theta & \theta + \theta^2 & 1 + \theta + \theta^2 & 1 + \theta^2 \\ 1 & \theta^2 & \theta + \theta^2 & 1 + \theta^2 & \theta & 1 + \theta & 1 + \theta + \theta^2 \\ 1 & 1 + \theta & 1 + \theta^2 & \theta^2 & 1 + \theta + \theta^2 & \theta & \theta + \theta^2 \\ 1 & \theta + \theta^2 & \theta & 1 + \theta + \theta^2 & \theta^2 & 1 + \theta^2 & 1 + \theta \\ 1 & 1 + \theta + \theta^2 & 1 + \theta & \theta & 1 + \theta^2 & \theta + \theta^2 & \theta^2 \end{bmatrix}$$

Now let H_0 be the first $n - k - \delta = 4$ rows of H and H_1 be the rest $\delta = 2$ rows. Then consider the convolutional code V with parity-check matrix

$$G(D) = H_0 + \tilde{H}_1 D$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \theta & \theta^2 & 1 + \theta & \theta + \theta^2 & 1 + \theta + \theta^2 & 1 + \theta^2 \\ 1+D & \theta^2+(\theta+\theta^2)D & (\theta+\theta^2)+\theta D & (1+\theta^2)+(1+\theta+\theta^2)D & \theta+\theta^2 D & (1+\theta)+(1+\theta^2)D & (1+\theta+\theta^2)+(1+\theta)D \\ 1+D & (1+\theta)+(1+\theta+\theta^2)D & (1+\theta^2)+(1+\theta)D & \theta^2+\theta D & (1+\theta+\theta^2)+(1+\theta^2)D & \theta+(\theta+\theta^2)D & (\theta+\theta^2)+\theta^2 D \end{bmatrix}$$

By (i) of Theorem 3 (i), V is a unit-memory MDS convolutional code with parameters $(7, 3, 2)_8$. The free distance of V is 7. Noting by (ii) and (iii) of Theorem 3, V has a maximal distance profile and is also strongly-MDS.

Example 3: MDS $(7, 4, 3)_8$

Here $k = 1, \delta = 3$. We use the cyclic code \mathcal{C} defined in **Example 2**, and we let H_0 be the first $n - k - \delta = 3$ rows of H and H_1 be the rest $\delta = 3$ rows of H where H is defined in **Example 2**. Then consider the convolutional code V with parity-check matrix

$$G(D) = H_0 + \tilde{H}_1 D$$

$$= \begin{bmatrix} 1+D & 1+(1+\theta)D & 1+(1+\theta^2)D & 1+\theta^2 D & 1+(1+\theta+\theta^2)D & 1+\theta D & 1+(\theta+\theta^2)D \\ 1+D & \theta+(\theta+\theta^2)D & \theta^2+\theta D & (1+\theta)+(1+\theta+\theta^2)D & (\theta+\theta^2)+\theta^2 D & (1+\theta+\theta^2)+(1+\theta^2)D & (1+\theta^2)+(1+\theta)D \\ 1+D & \theta^2+(1+\theta+\theta^2)D & (\theta+\theta^2)+(1+\theta)D & (1+\theta^2)+\theta D & \theta+(1+\theta^2)D & (1+\theta)+(\theta+\theta^2)D & (1+\theta+\theta^2)+\theta^2 D \end{bmatrix}$$

By Theorem 3 (i), V is a unit-memory MDS convolutional code with parameters $(7, 4, 3)_8$. The free distance of V is 7.

B. Case 2: $n = q = 8$

From Theorem 4, we use the \mathcal{GRS} codes $\mathcal{C}'_k = \mathcal{GRS}_k(\mathbf{v}, \mathbf{1})$, where $\mathbf{v} = (0, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6, \theta^7 = 1)$ and $\mathbf{1}$ is the all-one vector of length 8. Note that $\mathcal{C}'_k^\perp = \mathcal{GRS}_{8-k}(\mathbf{v}, \mathbf{1})$ and \mathcal{C}'_k is MDS with parameters $[8, k, 9 - k]_8$ for $1 \leq k \leq 8$.

Example 4: MDS $(8, 4, 2)_8$

Here $k = 2, \delta = 2$. A parity-check matrix H of \mathcal{C}'_2 is given by

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \theta & \theta^2 & \theta^3 & \theta^4 & \theta^5 & \theta^6 & 1 \\ 0 & \theta^2 & \theta^4 & \theta^6 & \theta^8 & \theta^{10} & \theta^{12} & 1 \\ 0 & \theta^3 & \theta^6 & \theta^9 & \theta^{12} & \theta^{15} & \theta^{18} & 1 \\ 0 & \theta^4 & \theta^8 & \theta^{12} & \theta^{16} & \theta^{20} & \theta^{24} & 1 \\ 0 & \theta^5 & \theta^{10} & \theta^{15} & \theta^{20} & \theta^{25} & \theta^{30} & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \theta & \theta^2 & 1+\theta & \theta+\theta^2 & 1+\theta+\theta^2 & 1+\theta^2 & 1 \\ 0 & \theta^2 & \theta+\theta^2 & 1+\theta^2 & \theta & 1+\theta & 1+\theta+\theta^2 & 1 \\ 0 & 1+\theta & 1+\theta^2 & \theta^2 & 1+\theta+\theta^2 & \theta & \theta+\theta^2 & 1 \\ 0 & \theta+\theta^2 & \theta & 1+\theta+\theta^2 & \theta^2 & 1+\theta^2 & 1+\theta & 1 \\ 0 & 1+\theta+\theta^2 & 1+\theta & \theta & 1+\theta^2 & \theta+\theta^2 & \theta^2 & 1 \end{bmatrix}$$

Now let H_0 be the first $q - k - \delta = 4$ rows of H and H_1 be the rest $\delta = 2$ rows but swapped in position. Then consider the convolutional code V with parity-check matrix

$$G(D) = H_0 + \tilde{H}_1 D$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \theta & \theta^2 & 1+\theta & \theta+\theta^2 & 1+\theta+\theta^2 & 1+\theta^2 & 1 \\ 0 & \theta^2+(1+\theta+\theta^2)D & (\theta+\theta^2)+(1+\theta)D & (1+\theta^2)+\theta D & \theta+(1+\theta^2)D & (1+\theta)+(\theta+\theta^2)D & (1+\theta+\theta^2)+\theta^2 D & 1+D \\ 0 & (1+\theta)+(\theta+\theta^2)D & (1+\theta^2)+\theta D & \theta^2+(1+\theta+\theta^2)D & (1+\theta+\theta^2)+\theta^2 D & \theta+(1+\theta^2)D & (\theta+\theta^2)+(1+\theta)D & 1+D \end{bmatrix}$$

By Theorem 4 (i), V is a unit-memory MDS convolutional code with parameters $(8, 4, 2)_8$. The free distance of V is 7. Noting that by (ii) and (iii) of Theorem 4, V has a maximal distance profile and is also strongly-MDS.

Example 5: MDS $(8, 5, 3)_8$

Here $k = 2, \delta = 3$. Let H_0 be the first $q - k - \delta = 3$ rows of H and H_1 be the rest $\delta = 3$ rows of H but reversed in position where H is defined in **Example 4**. Then consider the convolutional code V with parity-check matrix

$$G(D) = H_0 + \tilde{H}_1 D$$

$$= \begin{bmatrix} 1 & 1+(1+\theta+\theta^2)D & 1+(1+\theta)D & 1+\theta D & 1+(1+\theta^2)D & 1+(\theta+\theta^2)D & 1+\theta^2 D & 1+D \\ 0 & \theta+(\theta+\theta^2)D & \theta^2+\theta D & (1+\theta)+(1+\theta+\theta^2)D & (\theta+\theta^2)+\theta^2 D & (1+\theta+\theta^2)+(1+\theta^2)D & (1+\theta^2)+(1+\theta)D & 1+D \\ 0 & \theta^2+(1+\theta)D & (\theta+\theta^2)+(1+\theta^2)D & (1+\theta^2)+\theta^2 D & \theta+(1+\theta+\theta^2)D & (1+\theta)+\theta D & (1+\theta+\theta^2)+(\theta+\theta^2)D & 1+D \end{bmatrix}$$

By Theorem 4 (i), V is a unit-memory MDS convolutional code with parameters $(8, 5, 3)_8$. The free distance of V is 7.

Example 6: MDS $(8, 3, 2)_8$

Here $k = 1, \delta = 2$. A parity-check matrix H of \mathcal{C}'_1 is given by

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \theta & \theta^2 & \theta^3 & \theta^4 & \theta^5 & \theta^6 & 1 \\ 0 & \theta^2 & \theta^4 & \theta^6 & \theta^8 & \theta^{10} & \theta^{12} & 1 \\ 0 & \theta^3 & \theta^6 & \theta^9 & \theta^{12} & \theta^{15} & \theta^{18} & 1 \\ 0 & \theta^4 & \theta^8 & \theta^{12} & \theta^{16} & \theta^{20} & \theta^{24} & 1 \\ 0 & \theta^5 & \theta^{10} & \theta^{15} & \theta^{20} & \theta^{25} & \theta^{30} & 1 \\ 0 & \theta^6 & \theta^{12} & \theta^{18} & \theta^{24} & \theta^{30} & \theta^{36} & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \theta & \theta^2 & 1+\theta & \theta+\theta^2 & 1+\theta+\theta^2 & 1+\theta^2 & 1 \\ 0 & \theta^2 & \theta+\theta^2 & 1+\theta^2 & \theta & 1+\theta & 1+\theta+\theta^2 & 1 \\ 0 & 1+\theta & 1+\theta^2 & \theta^2 & 1+\theta+\theta^2 & \theta & \theta+\theta^2 & 1 \\ 0 & \theta+\theta^2 & \theta & 1+\theta+\theta^2 & \theta^2 & 1+\theta^2 & 1+\theta & 1 \\ 0 & 1+\theta+\theta^2 & 1+\theta & \theta & 1+\theta^2 & \theta+\theta^2 & \theta^2 & 1 \\ 0 & 1+\theta^2 & 1+\theta+\theta^2 & \theta+\theta^2 & 1+\theta & \theta^2 & \theta & 1 \end{bmatrix}$$

Now let H_0 be the first $q - k - \delta = 5$ rows of H and H_1 be the rest $\delta = 2$ rows but swapped in position. Then consider the convolutional code V with parity-check matrix

$$G(D) = H_0 + \tilde{H}_1 D$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \theta & \theta^2 & 1+\theta & \theta+\theta^2 & 1+\theta+\theta^2 & 1+\theta^2 & 1 \\ 0 & \theta^2 & \theta+\theta^2 & 1+\theta^2 & \theta & 1+\theta & 1+\theta+\theta^2 & 1 \\ 0 & (1+\theta)+(1+\theta^2)D & (1+\theta^2)+(1+\theta+\theta^2)D & \theta^2+(\theta+\theta^2)D & (1+\theta+\theta^2)+(1+\theta)D & \theta+\theta^2 D & (\theta+\theta^2)+\theta D & 1+D \\ 0 & (\theta+\theta^2)+(1+\theta+\theta^2)D & \theta+(1+\theta)D & (1+\theta+\theta^2)+\theta D & \theta^2+(1+\theta^2)D & (1+\theta^2)+(\theta+\theta^2)D & (1+\theta)+\theta^2 D & 1+D \end{bmatrix}$$

By Theorem 4 (i), V is a unit-memory MDS convolutional code with parameters $(8, 3, 2)_8$. The free distance of V is 8. By (ii) and (iii) of Theorem 4, V has a maximal distance profile and is also strongly-MDS.

Example 7: MDS $(8, 4, 3)_8$

Here $k = 1, \delta = 3$. Let H_0 be the first $q - k - \delta = 4$ rows of H and H_1 be the rest $\delta = 3$ rows of H but reversed in position where H is defined in **Example 6**. Then consider the convolutional code V with parity-check matrix

$$G(D) = H_0 + \tilde{H}_1 D$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \theta+(1+\theta^2)D & \theta^2+(1+\theta+\theta^2)D & (1+\theta)+(\theta+\theta^2)D & (\theta+\theta^2)+(1+\theta)D & (1+\theta+\theta^2)+\theta^2 D & (1+\theta^2)+\theta D & 1+D \\ 0 & \theta^2+(1+\theta+\theta^2)D & (\theta+\theta^2)+(1+\theta)D & (1+\theta^2)+\theta D & \theta+(1+\theta^2)D & (1+\theta)+(\theta+\theta^2)D & (1+\theta+\theta^2)+\theta^2 D & 1+D \\ 0 & (1+\theta)+(\theta+\theta^2)D & (1+\theta^2)+\theta D & \theta^2+(1+\theta+\theta^2)D & (1+\theta+\theta^2)+\theta^2 D & \theta+(1+\theta^2)D & (\theta+\theta^2)+(1+\theta)D & 1+D \end{bmatrix}$$

By Theorem 4 (i), V is a unit-memory MDS convolutional code with parameters $(8, 4, 3)_8$. The free distance of V is 8. By (ii) of Theorem 4, V has a maximal distance profile.

C. Case 3: $n = q + 1 = 9$

We shall use either **Construction one** or **two** in part 1 of Section V when $k \equiv q \pmod{2}$ and part 2 of Section V when $k \equiv q + 1 \pmod{2}$. We still use the same θ as in Cases 1 and 2, and let γ be a root of the polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$. Then θ has degree 3 over \mathbb{F}_2 , while γ has degree 2 over \mathbb{F}_2 . Hence the field $\mathbb{F}_2(\theta, \gamma)$ has degree 6 over \mathbb{F}_2 , i.e. it is isomorphic to \mathbb{F}_{64} .

Let $\beta = \theta(\theta + \gamma) \in \mathbb{F}_{64}^\times$. It can be easily seen that $\beta^2 = 1 + \theta\beta$, $\beta^3 = \theta + (1 + \theta^2)\beta$ and $\beta^9 = 1$, so the polynomial $f(x) = x^9 - 1 \in \mathbb{F}_8[x]$ has zeros exactly given by $\mathcal{Z}(f) = \{\beta^i : 0 \leq i \leq 8\}$.

Example 8: MDS $(9, 6, 2)_8$

Consider the cyclic code \mathcal{C} of length 9 over \mathbb{F}_8 with generator polynomial $h(x) = \prod_{i=-2}^2 (x - \beta^i)$. As a BCH code, this code is MDS with parameters $[9, 4, 6]_8$. We use **Construction one** in this case, and we have $k = 4$ and $\delta = 1$.

To give a parity-check matrix of \mathcal{C} , we start from the matrix

$$\overline{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \beta^7 & \beta^8 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta^8 & \beta^{10} & \beta^{12} & \beta^{14} & \beta^{16} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & 1+\theta\beta & \theta+(1+\theta^2)\beta & (1+\theta^2)+(1+\theta)\beta & (1+\theta)+(1+\theta)\beta & (1+\theta)+(1+\theta^2)\beta & (1+\theta^2)+\theta\beta & \theta+\beta \\ 1 & 1+\theta\beta & (1+\theta^2)+(1+\theta)\beta & (1+\theta)+(1+\theta^2)\beta & \theta+\beta & \beta & \theta+(1+\theta^2)\beta & (1+\theta)+(1+\theta)\beta & (1+\theta^2)+\theta\beta \end{bmatrix}$$

$$= \begin{bmatrix} \underline{k}_{1;0} \\ \underline{k}_{1;1} + \underline{k}_{1;-1}\beta \\ \underline{k}_{1;2} + \underline{k}_{1;-2}\beta \end{bmatrix}$$

where each $\underline{k}_{1;i} \in \mathbb{F}_8^9$, $-2 \leq i \leq 2$ since $\{1, \beta\}$ is a basis of $\mathbb{F}_{64} = \mathbb{F}_8(\beta)$ over \mathbb{F}_8 . A parity-check matrix of \mathcal{C} is given by

$$H = \begin{bmatrix} \underline{k}_{1;0} \\ \underline{k}_{1;1} \\ \underline{k}_{1;-1} \\ \underline{k}_{1;2} \\ \underline{k}_{1;-2} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \theta & 1+\theta^2 & 1+\theta & 1+\theta & 1+\theta^2 & \theta \\ 0 & 1 & \theta & 1+\theta^2 & 1+\theta & 1+\theta & 1+\theta^2 & \theta & 1 \\ 1 & 1 & 1+\theta^2 & 1+\theta & \theta & 0 & \theta & 1+\theta & 1+\theta^2 \\ 0 & \theta & 1+\theta & 1+\theta^2 & 1 & 1 & 1+\theta^2 & 1+\theta & \theta \end{bmatrix}.$$

Let H_0 be the first 3 rows of H and H_1 be the rest 2 rows. Consider the convolutional code V with parity-check matrix

$$H(D) = H_0 + \tilde{H}_1 D = \begin{bmatrix} \underline{k}_{1;0} \\ \underline{k}_{1;1} + \underline{k}_{1;2}D \\ \underline{k}_{1;-1} + \underline{k}_{1;-2}D \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1+D & D & 1+(1+\theta^2)D & \theta+(1+\theta)D & (1+\theta^2)+\theta D & 1+\theta & (1+\theta)+\theta D & (1+\theta^2)+(1+\theta)D & \theta+(1+\theta^2)D \\ 0 & 1+\theta D & \theta+(1+\theta)D & (1+\theta^2)+(1+\theta^2)D & (1+\theta)+D & (1+\theta)+D & (1+\theta^2)+(1+\theta^2)D & \theta+(1+\theta)D & 1+\theta D \end{bmatrix}$$

By Theorem 5, V is strongly-MDS with parameters $(9, 6, 2)_8$ and also has a maximal distance profile. The free distance of V is 6.

Example 9: MDS $(9, 5, 3)_8$

Let \mathcal{C} be the cyclic code of length 9 over \mathbb{F}_8 with generator polynomial $h(x) = \prod_{i=-3}^3 (x - \beta^i)$. This is a BCH code, and it is MDS with parameters $[9, 2, 8]_8$. We use **Construction two** in this case, and we have $\tau = 3$.

To give a parity-check matrix of \mathcal{C} , we start from the matrix

$$\begin{aligned} \overline{H} &= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \beta^7 & \beta^8 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta^8 & \beta^{10} & \beta^{12} & \beta^{14} & \beta^{16} \\ 1 & \beta^3 & \beta^6 & \beta^9 & \beta^{12} & \beta^{15} & \beta^{18} & \beta^{21} & \beta^{24} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & 1+\theta\beta & \theta+(1+\theta^2)\beta & (1+\theta^2)+(1+\theta)\beta & (1+\theta)+(1+\theta)\beta & (1+\theta)+(1+\theta^2)\beta & (1+\theta^2)+\theta\beta & \theta+\beta \\ 1 & 1+\theta\beta & (1+\theta^2)+(1+\theta)\beta & (1+\theta)+(1+\theta^2)\beta & \theta+\beta & \beta & \theta+(1+\theta^2)\beta & (1+\theta)+(1+\theta)\beta & (1+\theta^2)+\theta\beta \\ 1 & \theta+(1+\theta^2)\beta & (1+\theta)+(1+\theta^2)\beta & 1 & \theta+(1+\theta^2)\beta & (1+\theta)+(1+\theta^2)\beta & 1 & \theta+(1+\theta^2)\beta & (1+\theta)+(1+\theta^2)\beta \end{bmatrix} \\ &= \begin{bmatrix} \underline{k}_{1;0} \\ \underline{k}_{1;1} + \underline{k}_{1;-1}\beta \\ \underline{k}_{1;2} + \underline{k}_{1;-2}\beta \\ \underline{k}_{1;3} + \underline{k}_{1;-3}\beta \end{bmatrix}, \end{aligned}$$

where each $\underline{k}_{1;i} \in \mathbb{F}_8^9$, $-3 \leq i \leq 3$. Here the first index is kept as 1 since essentially those vectors for $-2 \leq i \leq 2$ are the same as those in **Example 8**.

As $\{1, \beta\}$ is a basis of $\mathbb{F}_{64} = \mathbb{F}_8(\beta)$ over \mathbb{F}_8 , a parity-check matrix of \mathcal{C} is given by

$$H = \begin{bmatrix} \underline{k}_{1;0} \\ \underline{k}_{1;1} \\ \underline{k}_{1;-1} \\ \underline{k}_{1;2} \\ \underline{k}_{1;-2} \\ \underline{k}_{1;3} \\ \underline{k}_{1;-3} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \theta & 1+\theta^2 & 1+\theta & 1+\theta & 1+\theta^2 & \theta \\ 0 & 1 & \theta & 1+\theta^2 & 1+\theta & 1+\theta & 1+\theta^2 & \theta & 1 \\ 1 & 1 & 1+\theta^2 & 1+\theta & \theta & 0 & \theta & 1+\theta & 1+\theta^2 \\ 0 & \theta & 1+\theta & 1+\theta^2 & 1 & 1 & 1+\theta^2 & 1+\theta & \theta \\ 1 & \theta & 1+\theta & 1 & \theta & 1+\theta & 1 & \theta & 1+\theta \\ 0 & 1+\theta^2 & 1+\theta^2 & 0 & 1+\theta^2 & 1+\theta^2 & 0 & 1+\theta^2 & 1+\theta^2 \end{bmatrix}$$

Let $H_0 = \begin{bmatrix} \underline{k}_{1;1} \\ \underline{k}_{1;-1} \\ \underline{k}_{1;3} \\ \underline{k}_{1;-3} \end{bmatrix}$ and $H_1 = \begin{bmatrix} \underline{k}_{1;0} \\ \underline{k}_{1;2} \\ \underline{k}_{1;-2} \end{bmatrix}$. Consider the convolutional code V with parity-check matrix

$$H(D) = H_0 + \tilde{H}_1 D = \begin{bmatrix} \underline{k}_{1;1} \\ \underline{k}_{1;-1} + \underline{k}_{1;0} D \\ \underline{k}_{1;3} + \underline{k}_{1;2} D \\ \underline{k}_{1;-3} + \underline{k}_{1;-2} D \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 1 & \theta & 1+\theta^2 & 1+\theta & 1+\theta & 1+\theta^2 & \theta \\ D & 1+D & \theta+D & (1+\theta^2)+D & (1+\theta)+D & (1+\theta)+D & (1+\theta^2)+D & \theta+D & 1+D \\ 1+D & \theta+D & (1+\theta)+(1+\theta^2)D & 1+(1+\theta)D & \theta+\theta D & 1+\theta & 1+\theta D & \theta+(1+\theta)D & (1+\theta)+(1+\theta^2)D \\ 0 & (1+\theta^2)+\theta D & (1+\theta^2)+(1+\theta)D & (1+\theta^2)D & (1+\theta^2)+D & (1+\theta^2)+D & (1+\theta^2)D & (1+\theta^2)+(1+\theta)D & (1+\theta^2)+\theta D \end{bmatrix}$$

By Theorem 6, V is MDS with parameters $(9, 5, 3)_8$. The free distance of V is 8. Since the block code with parity-check matrix H_0 is MDS, the code V also has a maximal distance profile.

Example 10: MDS $(9, 3, 2)_8$

Since $k = 1$ is not congruent to q modulo 2, we use $f(x) = x^9 - \alpha^9 \in \mathbb{F}_8[x]$, so its set of zeros is exactly $\mathcal{Z}(f) = \{\alpha\beta^i : 0 \leq i \leq 8\}$. Hence the block codes we consider are constacyclic codes of length 9 over \mathbb{F}_8 . Here α can be taken to be any primitive element of \mathbb{F}_{64} such that $\alpha^7 = \beta$. In particular, since $\theta + \gamma$ is a primitive element of \mathbb{F}_{64} and $(\theta + \gamma)^7 = (\theta^{-1}\beta)^7 = \beta^7$, so that $[(\theta + \gamma)^4]^7 = \beta$, we may take $\alpha = (\theta + \gamma)^4 = \theta^2 + (1 + \theta^2)\beta \in \mathbb{F}_{64}^\times$.

Consider the constacyclic code $\mathcal{C} \subset \mathbb{F}_8[x]/(f(x))$ of length 9 over \mathbb{F}_8 with generator polynomial $h(x) = \prod_{i=-3}^4 (x - \alpha\beta^i)$. By Lemma 2, this code is MDS with parameters $[9, 1, 9]_8$. We have $k = 1$ and $\delta = 1$.

To give a parity-check matrix of \mathcal{C} , we start from the matrix

$$\overline{H} = \begin{bmatrix} 1 & \alpha\beta & (\alpha\beta)^2 & (\alpha\beta)^3 & (\alpha\beta)^4 & (\alpha\beta)^5 & (\alpha\beta)^6 & (\alpha\beta)^7 & (\alpha\beta)^8 \\ 1 & \alpha\beta^2 & (\alpha\beta^2)^2 & (\alpha\beta^2)^3 & (\alpha\beta^2)^4 & (\alpha\beta^2)^5 & (\alpha\beta^2)^6 & (\alpha\beta^2)^7 & (\alpha\beta^2)^8 \\ 1 & \alpha\beta^3 & (\alpha\beta^3)^2 & (\alpha\beta^3)^3 & (\alpha\beta^3)^4 & (\alpha\beta^3)^5 & (\alpha\beta^3)^6 & (\alpha\beta^3)^7 & (\alpha\beta^3)^8 \\ 1 & \alpha\beta^4 & (\alpha\beta^4)^2 & (\alpha\beta^4)^3 & (\alpha\beta^4)^4 & (\alpha\beta^4)^5 & (\alpha\beta^4)^6 & (\alpha\beta^4)^7 & (\alpha\beta^4)^8 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & (1+\theta^2)+(1+\theta^2)\beta & (1+\theta^2)\beta & (1+\theta+\theta^2)+\theta\beta & (1+\theta+\theta^2)+(1+\theta^2)\beta & 1+\theta^2\beta & (1+\theta+\theta^2)+(1+\theta)\beta & \theta+\beta & \theta^2+(1+\theta^2)\beta \\ 1 & (1+\theta^2)+\theta^2\beta & 1+(1+\theta+\theta^2)\beta & \theta^2 & \theta+(\theta+\theta^2)\beta & \theta^2+\beta & \theta+\theta^2 & (1+\theta)+(1+\theta^2)\beta & (\theta+\theta^2)+\theta^2\beta \\ 1 & \theta^2+(\theta+\theta^2)\beta & \theta^2+\theta^2\beta & (1+\theta)+\theta\beta & (1+\theta+\theta^2)\beta & \theta^2+\theta\beta & 1+(1+\theta)\beta & (1+\theta^2)+(1+\theta)\beta & (1+\theta)+(\theta+\theta^2)\beta \\ 1 & (\theta+\theta^2)+(1+\theta)\beta & (1+\theta+\theta^2)+\beta & (1+\theta+\theta^2)+\theta\beta & \theta+\theta\beta & 1+(\theta+\theta^2)\beta & (1+\theta+\theta^2)+(1+\theta)\beta & 1+\theta\beta & (1+\theta)\beta \end{bmatrix}$$

$$= \begin{bmatrix} \underline{k}_{3;1} + \underline{k}_{3;0}\beta \\ \underline{k}_{3;2} + \underline{k}_{3;-1}\beta \\ \underline{k}_{3;3} + \underline{k}_{3;-2}\beta \\ \underline{k}_{3;4} + \underline{k}_{3;-3}\beta \end{bmatrix}$$

where each $\underline{k}_{3;i} \in \mathbb{F}_8^9$, $-3 \leq i \leq 4$. As $\{1, \beta\}$ is a basis of $\mathbb{F}_{64} = \mathbb{F}_8(\beta)$ over \mathbb{F}_8 , a parity-check matrix of \mathcal{C} is given by

$$H = \begin{bmatrix} \underline{k}_{3;1} \\ \underline{k}_{3;0} \\ \underline{k}_{3;2} \\ \underline{k}_{3;-1} \\ \underline{k}_{3;3} \\ \underline{k}_{3;-2} \\ \underline{k}_{3;4} \\ \underline{k}_{3;-3} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1+\theta^2 & 0 & 1+\theta+\theta^2 & 1+\theta+\theta^2 & 1 & 1+\theta+\theta^2 & \theta & \theta^2 \\ 0 & 1+\theta^2 & 1+\theta^2 & \theta & 1+\theta^2 & \theta^2 & 1+\theta & 1 & 1+\theta^2 \\ 1 & 1+\theta^2 & 1 & \theta^2 & \theta & \theta^2 & \theta+\theta^2 & 1+\theta & \theta+\theta^2 \\ 0 & \theta^2 & 1+\theta+\theta^2 & 0 & \theta+\theta^2 & 1 & 0 & 1+\theta^2 & \theta^2 \\ 1 & \theta^2 & \theta^2 & 1+\theta & 0 & \theta^2 & 1 & 1+\theta^2 & 1+\theta \\ 0 & \theta+\theta^2 & \theta^2 & \theta & 1+\theta+\theta^2 & \theta & 1+\theta & 1+\theta & \theta+\theta^2 \\ 1 & \theta+\theta^2 & 1+\theta+\theta^2 & 1+\theta+\theta^2 & \theta & 1 & 1+\theta+\theta^2 & 1 & 0 \\ 0 & 1+\theta & 1 & \theta & \theta & \theta+\theta^2 & 1+\theta & \theta & 1+\theta \end{bmatrix}$$

Now let H_0 be the first 6 rows of H and H_1 be the rest 2 rows. Consider the convolutional code V with parity-check matrix

$$H(D) = H_0 + \tilde{H}_1 D = \begin{bmatrix} \underline{k}_{3;1} \\ \underline{k}_{3;0} \\ \underline{k}_{3;2} \\ \underline{k}_{3;-1} \\ \underline{k}_{3;3} + \underline{k}_{3;4}D \\ \underline{k}_{3;-2} + \underline{k}_{3;-3}D \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1+\theta^2 & 0 & 1+\theta+\theta^2 & 1+\theta+\theta^2 & 1 & 1+\theta+\theta^2 & \theta & \theta^2 \\ 0 & 1+\theta^2 & 1+\theta^2 & \theta & 1+\theta^2 & \theta^2 & 1+\theta & 1 & 1+\theta^2 \\ 1 & 1+\theta^2 & 1 & \theta^2 & \theta & \theta^2 & \theta+\theta^2 & 1+\theta & \theta+\theta^2 \\ 0 & \theta^2 & 1+\theta+\theta^2 & 0 & \theta+\theta^2 & 1 & 0 & 1+\theta^2 & \theta^2 \\ 1+D & \theta^2+(\theta+\theta^2)D & \theta^2+(1+\theta+\theta^2)D & (1+\theta)+(1+\theta+\theta^2)D & \theta D & \theta^2+D & 1+(1+\theta+\theta^2)D & (1+\theta^2)+D & 1+\theta \\ 0 & (\theta+\theta^2)+(1+\theta)D & \theta^2+D & \theta+\theta D & (1+\theta+\theta^2)+\theta D & \theta+(\theta+\theta^2)D & (1+\theta)+(1+\theta)D & (1+\theta)+\theta D & (\theta+\theta^2)+(1+\theta)D \end{bmatrix}$$

By Theorem 7, V is strongly-MDS with parameters $(9, 3, 2)_8$ and also has a maximal distance profile. The free distance of V is 9.

Example 11: MDS $(9, 4, 2)_8$

We use the cyclic code \mathcal{C} as in **Example 9**, but we instead use **Construction one** in this case. We have $k = 2$ and $\delta = 1$.

We let H_0 be the first 5 rows of H and H_1 be the rest 2 rows. Consider the convolutional code V with parity-check matrix

$$H(D) = H_0 + \tilde{H}_1 D = \begin{bmatrix} \underline{k}_{1;0} \\ \underline{k}_{1;1} \\ \underline{k}_{1;-1} \\ \underline{k}_{1;2} + \underline{k}_{1;3}D \\ \underline{k}_{1;-2} + \underline{k}_{1;-3}D \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \theta & 1+\theta^2 & 1+\theta & 1+\theta & 1+\theta^2 & \theta \\ 0 & 1 & \theta & 1+\theta^2 & 1+\theta & 1+\theta & 1+\theta^2 & \theta & 1 \\ 1+D & 1+\theta D & (1+\theta^2)+(1+\theta)D & (1+\theta)+D & \theta+\theta D & (1+\theta)D & \theta+D & (1+\theta)+\theta D & (1+\theta^2)+(1+\theta)D \\ 0 & \theta+(1+\theta^2)D & (1+\theta)+(1+\theta^2)D & 1+\theta^2 & 1+(1+\theta^2)D & 1+(1+\theta^2)D & 1+\theta^2 & (1+\theta)+(1+\theta^2)D & \theta+(1+\theta^2)D \end{bmatrix}$$

By Theorem 5, V is strongly-MDS with parameters $(9, 4, 2)_8$ and also has a maximal distance profile. The free distance of V is 8.

VII. CONCLUSION

Maximum-distance separable (MDS) convolutional codes are characterized by the property that the free distance attains the generalized Singleton bound. Thus MDS convolutional codes form an optimal family of convolutional codes, the study of which is of great importance. There are very few general algebraic constructions of MDS convolutional codes. In this paper, we construct a large family of unit-memory MDS convolutional code over \mathbb{F}_q of length $n \leq q + 1$ with flexible parameters. Compared with previous works, the field size q required to define these codes is much smaller. The construction also leads to many new strongly-MDS convolutional codes, an important subclass of MDS convolutional codes proposed and studied in [8]. At the end of the paper we present many examples to illustrate the construction.

Acknowledgment

The research of M. Xiong was supported by RGC grant number 606211 and 609513 from Hong Kong.

REFERENCES

- [1] S. A. Aly, M. Grassl, A. Klappenecker, M. Rötteler, and P. K. Sarvepalli, "Quantum convolutional BCH codes," in *Proc. IEEE 10th CWIT*, pp. 180–183, 2007.
- [2] J. Chen, J. Li, Y. Huang, J. Lin, "Some families of asymmetric quantum codes and quantum convolutional codes from constacyclic codes," *Linear Algebra Appl.* vol. 475, pp. 186–199, 2015.
- [3] W. Ebel, "A directed search approach for unit-memory convolutional codes," *IEEE Trans. Inform. Theory*, vol. 42, no. 4, pp. 1290–1297, 1996.
- [4] P. Elias, "Coding for noisy channels," *IRE Conv. Rep.*, Pt. 4, pp. 37–47, 1955.
- [5] G. G. La Guardia, "On nonbinary quantum convolutional BCH codes," *Quantum Inf. Comput.* vol. 12, no. 9-10, pp. 820–842, 2012.
- [6] G. G. La Guardia, "On classical and quantum MDS-convolutional BCH codes," *IEEE Trans. Inform. Theory*, vol. 60, no. 1, pp. 304–312, 2014.
- [7] G. G. La Guardia, "On Negacyclic MDS-Convolutional Codes," *Linear Algebra Appl.*, vol. 448, pp. 85–96, 2014.
- [8] H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache, "Strongly-MDS convolutional codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 2, pp. 584–598, 2006.
- [9] C. N. Hadjicostis, "Nonconcurrent error detection and correction in fault-tolerant discrete-time LTI dynamic systems," *IEEE Trans. Circuits Syst. I*, vol. 50, no. 1, pp. 45–55, 2003.
- [10] C. N. Hadjicostis, "Finite-state machine embeddings for nonconcurrent error detection and identification encoded dynamics for fault tolerance in linear finite-state machines," *IEEE Trans. Autom. Control*, vol. 50, no. 2, pp. 142–153, 2005.
- [11] C. N. Hadjicostis and G. C. Verghese, "Encoded dynamics for fault tolerance in linear finite-state machines," *IEEE Trans. Autom. Control*, vol. 47, no. 1, pp. 189–192, 2002.
- [12] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.
- [13] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding*. Piscataway, NJ: IEEE Press, 1999.
- [14] J. Justesen, "An algebraic construction of rate $1/v$ convolutional codes," *IEEE Trans. Inform. Theory*, vol. IT-21, no. 1, pp. 577–580, 1975.
- [15] L. N. Lee, "Short unit-memory byte-oriented binary convolutional codes having maximal free distance," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 349–352, 1976.
- [16] S. Li, M. Xiong and G. Ge, "Cyclic Codes of General Type and the Construction of Quantum MDS Codes," preprint.
- [17] R. J. McEliece, "The algebraic theory of convolutional codes," in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, vol. 1, pp. 1065–1138.
- [18] P. Piret, *Convolutional Codes, an Algebraic Approach*. Cambridge, MA: MIT Press, 1988.
- [19] J. Rosenthal and R. Smarandache, "Maximum distance separable convolutional codes," *Appl. Algebra Engrg. Comm. Comput.*, vol. 10, pp. 15–32, 1999.
- [20] R. Smarandache, *Maximum distance separable convolutional codes, construction and decoding*, Ph.D thesis, Department of Mathematics, University of Notre Dame, 2001.
- [21] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal, "Constructions for MDS-convolutional codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 5, pp. 2045–2049, 2001.
- [22] C. Thommesen and J. Justesen, "Bounds on distances and error exponents of unit memory codes," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 5, pp. 637–649, 1983.
- [23] A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," *IEEE Trans. Inform. Theory*, IT-13:260–269, 1967.
- [24] T. Yan, X. Huang, Y. Tang, "Quantum convolutional codes derived from constacyclic codes," *Modern Phys. Lett. B* vol. 28, no. 31, 1450241, 15 pp, 2014.
- [25] G. Zhang, B. Chen, L. Li, "A Construction of MDS Quantum Convolutional Codes," *Internat. J. Theoret. Phys.* vol. 54, no. 9, pp. 3182–3194, 2015.